مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates - Microsoft

Tracking #:432317685

Date:10-09-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Microsoft has released its September 2025 Patch Tuesday updates, addressing 86 vulnerabilities across Windows, Office, Hyper-V, SMB, NTLM, and related components.

TECHNICAL DETAILS:

Microsoft has released its September 2025 Patch Tuesday updates, addressing 86 vulnerabilities across Windows, Office, Hyper-V, SMB, NTLM, and related components. The update includes:

- **2 publicly disclosed zero-day vulnerabilities** (SMB and Newtonsoft.Json).
- **8 Critical vulnerabilities**, several with **remote code execution (RCE)** potential.

No vulnerabilities are confirmed as actively exploited in the wild at the time of release. However, several are marked **"exploitation more likely"** by Microsoft, making rapid remediation a priority.

Publicly Disclosed Zero-Days

1. **CVE-2025-55234 – Windows SMB EoP (CVSS 8.8)**

- Allows unauthenticated remote attackers to perform relay attacks against SMB servers without signing/EPA enabled.
- Exploitation more likely.

2. **CVE-2024-21907 – Newtonsoft.Json DoS in SQL Server (CVSS 7.5)**

- Improper handling of crafted JSON payloads causes denial of service in SQL Server.
- Exploitation less likely.

Critical Vulnerabilities:

- CVE-2025-54916 – Windows NTFS RCE (CVSS 8.8)
  Stack buffer overflow enabling network-based RCE across multiple Windows versions.
- CVE-2025-54910 – Microsoft Office RCE (CVSS 8.4)
  Heap overflow allowing arbitrary code execution via crafted documents; exploitable via Preview Pane.
- CVE-2025-54918 – Windows NTLM EoP (CVSS 8.8)
  Improper NTLM authentication enables SYSTEM privilege escalation over the network.
- CVE-2025-54101 – Windows SMB v3 Client/Server RCE
  Race condition leading to remote code execution with authenticated access.
- CVE-2025-55228, CVE-2025-53800, CVE-2025-55236 – Graphics/Win32K Kernel
  Enable local privilege escalation and possible Hyper-V guest-to-host escapes.
- CVE-2025-55224 – Hyper-V RCE (CVSS 7.8)
  Local attacker in guest VM may escape into the host system.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently released by Microsoft.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://msrc.microsoft.com/update-guide/releaseNote/2025-Sep